

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

-----X	
SONAL BOSE, Individually, on Behalf of	:
Herself and All Others Similarly Situated,	:
	:
Plaintiff,	:
	:
v.	:
	:
INTERCLICK, INC.; MCDONALD’S USA,	:
LLC; MCDONALD’S CORPORATION;	:
CBS CORPORATION; MAZDA MOTOR	:
OF AMERICA, INC.; MICROSOFT	:
CORPORATION; and DOES 1-50,	:
	:
Defendants.	:
-----X	

**10 Civ. 9183 (DAB)**  
  
**FIRST AMENDED**  
**CLASS ACTION COMPLAINT**  
  
**DEMAND FOR JURY TRIAL**

Plaintiff, individually and on behalf of all others similarly situated, makes the following allegations based on her personal knowledge of her own acts and observations and, otherwise, upon information and belief based on investigation of counsel.

# **I. NATURE OF THE CASE**

1. In this complaint, Plaintiff alleges that Defendant Interclick, a web ad-serving company, monitored her web browsing in ways she would not expect or detect.

2. In particular, to circumvent measures Plaintiff took to prevent such monitoring, Interclick served online advertisements that included hidden code to “sniff” Plaintiff’s browser history and to deposit Adobe Flash local shared objects on her computer to monitor her online activities on an ongoing basis.

3. Plaintiff alleges that Defendants invaded her privacy, misappropriated her personal information, and interfered with the operability of her computer—conduct and consequences for which she now seeks relief.

4. While visiting websites that displayed Defendants' advertisements, Defendants used their ad displays as a cover for mining Plaintiff's computer to identify websites she had previously visited.

5. All Defendants worked together in a common exercise for their mutual benefit, playing their respective roles in advertising campaigns, mining consumers' web browser histories for entries of particular relevance to Defendants' respective, customized advertising campaigns and, to the same end, setting Adobe LSOs ("Flash cookies") as cookie substitutes outside the purview of consumers' cookie-based privacy and security controls.

6. Defendants circumvented the privacy and security controls of consumers who, like Plaintiff, had configured their browsers to prevent third-party advertisers from monitoring their online activities.

## **II. PARTIES**

7. Ms. Bose ("Plaintiff") is a resident of the City, County, and State of New York.

8. Defendant interCLICK, Inc. ("Interclick"), operates an online advertising network. Interclick is a Delaware Corporation with corporate headquarters at 257 Park Avenue South, Sixth Floor, New York, New York 10010.

9. Defendant McDonald's USA, LLC operates and franchises McDonald's restaurants in the United States. McDonald's USA, LLC is a Delaware corporation with principal offices at One McDonald's Plaza, Oak Brook, Illinois 60523 and is a subsidiary of McDonald's Corporation. McDonald's USA, LLC's registered agent for service of process is Illinois Corporation Service Company, One Adlai Stevenson Drive, Springfield, Illinois 62703.

10. Defendant McDonald's Corporation is the parent company of McDonald's USA, LLC and other non-U.S. subsidiaries. McDonald's Corporation is the owner and operator of the

website identified by the domain name, “www.mcdonalds.com.” In McDonald’s Corporation’s 2010 U.S. Securities and Exchange Commission Form 10-K, McDonald’s Corporation refers to itself and its subsidiaries, collectively, as “McDonald’s,” without materially distinguishing between the its and its subsidiaries business functions. For purposes of this complaint, McDonald’s Corporation and McDonald’s USA, LLC are referred to herein collectively as “McDonald’s.”

11. Defendant Microsoft Corporation (“Microsoft”) creates and licenses a wide array of software products and services ranging from operating systems, browsers, and online services, and sells devices that include gaming consoles and mobile telephones. Microsoft is a Washington corporation with principal offices at One Microsoft Way, Redmond, Washington.

12. Defendant CBS Corporation (“CBS Sportsline”) is the ultimate owner and operator of CBS Sports/SportsLine.com, Inc., a provider of online, sports-related information and entertainment. CBS Corporation is a Delaware corporation with principal offices at 51 West 52nd Street, New York, New York 10019.

13. Defendant Mazda Motor of America, Inc. (“Mazda”) oversees the sales, marketing, parts, and customer service support activities of hundreds of Mazda dealers in the U.S. and other North American countries. Mazda is the United States subsidiary of Mazda Motor Corporation, a Japanese corporation, and is headquartered at 7755 Irvine Center Drive, Irvine, California 92618.

14. Each of the defendants designated as Does 1-50 (“Does”) is an individual, corporation, or other business or legal entity, the actual name and location of which is unknown to Plaintiff. Plaintiff designates each such defendant by a fictitious “Doe” name and alleges that, during the Class Period (defined below), each Doe defendant engaged in conduct of a character and consequence like the conduct Plaintiff attributes to the defendants specifically named above.

For Doe defendants whose actual identities Plaintiff discovers, Plaintiff will name such defendants by amending her complaint filed in this matter, as permitted by the Court.

15. The defendants named and designated above are collectively referred to in this complaint as “Defendants.”

### **III. JURISDICTION AND VENUE**

16. This Court has subject-matter jurisdiction over the this action pursuant to Title 28, United States Code, Section 1332, as amended by the Class Action Fairness Act of 2005, in that (a) the aggregate claims of Plaintiffs and the proposed Class Members exceed the sum or value of \$5,000,000, exclusive of interest and costs; (b) minimal diversity of citizenship exists between the proposed Class Members and Defendants; and (c) the Classes each consist of more than one hundred members.

17. This Court has federal subject-matter jurisdiction over this action pursuant to Title 28, United States Code, Section 1331 as this action arises in part under a federal statute.

18. This Court has supplemental jurisdiction with respect to the pendent state law claims under Title 28, United States Code, Section 1367.

19. Venue is proper in this District under Title 28, United States Code, Section 1391(b) because Defendants’ improper conduct alleged in this complaint occurred in, was directed from, and/or emanated from this judicial district, including through the actions of Manhattan-based interCLICK, Inc. that are alleged in this complaint.

### **IV. FACTUAL ALLEGATIONS**

#### **A. Interclick’s Business**

20. Interclick is an online advertising network and services provider with principal offices at 257 Park Avenue South, Sixth Floor, New York, New York 10010.

21. Interclick earns its revenue from advertiser (or ad agency) clients that pay Interclick to display their advertisements on web pages.

22. For the month of December 2009, comScore Media Metrix ranked Interclick 10th among U.S. Internet ad networks, with an audience of approximately 149 million unique users, over 72 percent of the total Internet audience that month.

23. When a consumer visits a web page that includes a third-party advertisement, the display of the advertisement occurs because the web page causes the consumer to communicate with the ad network's systems; thus, Interclick's "audience" consists of consumers who visited websites on which Interclick displayed its clients' advertisements, not consumers who chose to communicate with Interclick or necessarily knew of Interclick's existence.

24. Interclick delivers its clients' advertisement on an ad network consisting of websites, or "publishers," which Interclick pays for their inventory. "Inventory" is advertising display space on a web pages.

25. The inventory Interclick purchases from websites is remnant inventory, also called "non-premium" inventory. After websites sell their premium inventory—which they typically sell directly to advertisers, with guarantees regarding factors such as ad placement, times of day, and volume of traffic—the remaining, unsold inventory is remnant inventory.

26. For premium inventory, advertisers typically pay based on CPMs (cost per thousand ad views).

27. For delivering their ads on remnant inventory, advertisers pay Interclick performance-based fees.

28. Performance-based fees vary based on how the consumer viewing an ad responds, for example, by mousing over the ad, clicking on it, or clicking through to complete a purchase transaction.

**B. Defendants's Flash LSO Exploit**

29. Because Defendants's derives its revenue primarily from performance-based fees, Defendants tries to maximize "return on ad spend" by engaging in behavioral targeting.

30. Like many online, third-party services, Defendants tracks consumers by depositing and reading browser cookies containing unique identifiers and browsing history information that it uses to create behavioral profiles; when a profiled consumer visits a web page on which Defendants serves advertisements, Defendants uses the profile to select particular categories of ads with which to target the user.

31. A consumer who does not want to be tracked by third parties such as Defendants can set her browser controls to block third-party cookies. For example, in Safari, this control is accessed as follows:

*Safari > Preferences > Security > Accept cookies: Only from sites I visit / Block cookies from third parties and advertisers*

32. In addition, a consumer can delete browser cookies previously stored by third parties to attempt to prevent the third party from associating previously acquired tracking data with the consumer's subsequent web activity.

33. Mechanisms to block and delete third-party cookies are generally available to consumers using commercial browsers.

34. Defendants augmented its tracking technology by using tracking mechanisms that users could not reasonably block or delete: Defendants stored tracking data on consumers' computers in Adobe Flash local shared objects ("LSOs," sometimes referred to as "Flash cookies").

35. Adobe Flash Player is installed on the majority of U.S. consumers' computers.

36. LSOs are files designed to be used by consumers' Adobe Flash Player software, for purposes such as storing a consumer's volume control preference for audio content or retaining the score of a video game the consumer plays in multiple sessions.

37. Adobe Corporation has stated that LSOs were designed to support consumers' ability to experience "rich Internet application" content using the Adobe Flash Player. Letter to FTC, Adobe Systems Inc., Jan. 27, 2010, available at <http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf> (last accessed Dec. 6, 2010).

38. Defendants stored LSOs on consumers' computers for purposes other than delivering content to play on consumers' Flash Players or to retain settings for playing Flash content chosen by consumers.

39. Instead, Defendants used LSOs as a substitute and back-up for browser cookies so it could track, profile, and serve targeted advertisements to consumers without being subject to the controls consumers reasonably expected to have over such third-party interactions on the Internet: for consumers whose browser controls were set to block third-party cookies, Defendants used LSOs; and for consumers who had deleted Interclick's browser cookies, Defendants recreated the deleted browser cookies by using the contents stored in LSOs.

40. Interclick's use of this technology was independently confirmed in a report issued by academic researchers and titled, "Flash Cookies and Privacy," which found that a user visiting a website would receive a standard, browser cookie, and an identical, Interclick LSO or "Flash cookie;" if the user deleted the browser cookie, the LSO would be used to "re-spawn" the browser cookie; these operations happened without any notice to the user and without any con-

sent from the user; in addition, both the browser cookie and the LSO set by Interclick would contain a common user identifier. *See* “Flash Cookies and Privacy,” A. Soltani, S. Canty, Q. Mayo, L. Thomas, C.J. Hoofnagle, Univ. Cal., Berkeley, Aug. 10, 2009 at 3, available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1446862](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862) (last accessed Dec. 6, 2010).

41. In its letter to the Federal Trade Commission earlier this year, Adobe Systems Incorporated stated, “Adobe condemns the practice of using Local Storage to back up browser cookies for the purpose of restoring them later without user knowledge and express consent.” Letter to FTC, Adobe Systems Inc., Jan. 27, 2010, p. 9, available at <http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf> (last accessed Dec. 6, 2010).

42. Interclick reportedly claims it no longer uses LSOs for ad targeting.

43. For consumers, including Plaintiff and Class Members, on whose computers Interclick has deposited LSOs, those LSOs continue to reside and remain available to Interclick and its customers.

44. Unlike third-party browser cookies, for which commercial browsers provide consumers some measure of control, consumers have no reasonable means to decline, detect, or delete LSOs. To the extent Adobe is now providing a usable control mechanism: consumers are not generally aware of it, or the need for using it; even if consumers are aware, it is unreasonable to consumers with taking steps to protect themselves and, if they do not, leaving them to suffer intrusions that they would not be suffering but for the conduct of entities such as Defendants.

**C. Defendants' Browser-history sniffing Exploit**

45. In the course of displaying advertisements, Interclick executes program code that records the consumer's history of browsing of browsing websites other than the one on which Interclick displays ads to the consumer.

46. This technique of acquiring consumers' web activity data is known as "browser history sniffing" or a "history-sniffing attack." History sniffing exploits the standard browser function that causes a user's previously visited links to be displayed in a different color than links a user has not visited.

47. Interclick's purpose in performing history sniffing was to determine whether a consumer had previously visited certain web pages of particular interest to the advertiser Defendants and of particular utility in inferring behavioral interests and selecting an advertisement.

48. Interclick performed history-sniffing as follows: (a) in its code to display an advertisement to a consumer, Interclick embedded history-sniffing code invisible to the consumer; (b) the history-sniffing code contained a list of web page hyperlinks; (c) although the hyperlinks were not displayed to the consumer, the consumer's browser automatically assigned each link a color designation based on whether the user had previously visited the web page associated with the link; (d) the history-sniffing code performed an examination of the list of color-designated hyperlinks; (e) the history-sniffing code transmitted the results of this examination to Interclick's servers.

49. Interclick's use of this technology was independently confirmed in a report published by academic researchers. *See* "An Empirical Study of Privacy-Violating Information Flows in JavaScript Web Applications," D. Jang, R. Jhala, S. Lerner, H. Shacham, Univ. Cal.,

San Diego, Oct. 2010, sec. 4, available at <http://cseweb.ucsd.edu/~d1jang/papers/ccs10.pdf> (last accessed Dec. 6, 2010).

50. Research results showed that, on the web pages on which Interclick performed browser-history sniffing, Interclick's hidden list of hyperlinks contained links for as many 222 websites. *See id.*

51. Research results showed that Interclick performed browser-history sniffing to inspect for user visits to a variety of websites, including health, finance, and movie websites, and websites associated with Japanese *manga* publications and *anime* video productions popular with a U.S. audience that includes minors.<sup>1</sup> *See id.*

52. In the research results, Interclick was the entity most frequently associated with the browser-history sniffing. *See id.*

53. Browser sniffing constitutes cross-domain activity that violates global Internet standards.

---

<sup>1</sup> In early 2011, websites on which Interclick displayed ads included the following 66 sites:

ae.com	constantcontact.com	ipage.com	radaronline.com
aeropostale.com	couponcabin.com	kaspersky.com	readwriteweb.com
afterdawn.com	crateandbarrel.com	kodak.com	reference.com
ajc.com	csmonitor.com	landsend.com	register.com
allbusiness.com	cvs.com	logitech.com	sfgate.com
americangreetings.com	dailymail.co.uk	mangafox.com	staples.com
bebo.com	dealnews.com	manta.com	starwoodhotels.com
blockbuster.com	denverpost.com	mediotiempo.com	superpages.com
bloomingdales.com	dishnetwork.com	motortrend.com	tarot.com
bluemountain.com	dominos.com	musiciansfriend.com	tomshardware.com
borders.com	express.com	n4g.com	urbanoutfitters.com
bravenet.com	gigaom.com	nationalgeographic.com	verizonwireless.com
bravotv.com	glassdoor.com	nationalrail.co.uk	verticalresponse.com
businessinsider.com	grooveshark.com	netsuite.com	vistaprint.com
cabelas.com	howtoforge.com	nexon.net	washingtonpost.com
cheatcc.com	ibtimes.com	pordescargadirecta.com	
computing.net	icanhascheezburger.com	potterybarn.com	

**D. Defendants' Advertising Campaigns**

54. In mid-2010, McDonald's mounted a month-long online advertising campaign tied to its World Cup sponsorship and designed to increase consumer traffic on its website, where consumers could play an online, World Cup-themed game with prize chances. A participating consumer had to enter a unique, nine-digit code from a peel-off game piece acquired from the packaging of a McDonald's sandwich. In addition, each participating consumer had to provide personally identifying information to McDonald's, including name, date of birth, telephone number, mailing address, and email address. Consumers could also play the World Cup game on mobile phones served by one of 23 wireless carriers.

55. Before the spring 2010 start of the major league baseball season, CBS Sportsline promoted its online fantasy sports platform in an advertising campaign designed to improve its market share position against competitors by registering new users and re-engaging users who had previously registered.

56. In 2010, Mazda launched a two-month advertising campaign promoting its new models and summer sales events and designed to increase consumer traffic on its website and identify potential buyers.

57. In 2010, Microsoft mounted a seven-month advertising campaign to promote sales of its new Windows Smartphone.

**E. Defendants' Activities with Interclick**

58. To conduct these online advertising campaigns, each Defendant engaged Interclick.

59. Interclick specializes in "behavioral advertising," that is, Interclick tracks individual consumers to collect information about their web-browsing activities, which it compiles in

individual profiles and analyzes to determine which advertisements to display to which consumers.

60. Interclick and Defendants worked together in planning, executing, and monitoring the success of Defendants' respective online advertising campaigns. Interclick makes a particular point of touting its competitive advantage in the degree of control it provides clients, the real-time reporting and campaign adjustment from which its clients can expect to benefit, and the degree of consumer profile-based customization clients can expect based on Interclick's substantial data warehouse resources (discussed below).

#### **F. Interclick's "Enhancement" of Consumers' Information**

61. Interclick states that it "organizes and valuates billions of data points daily to construct the most responsive digital audiences for major digital marketers."

62. Interclick continually updates its database of consumer profiles with information acquired from and about consumers in its online advertising campaigns.

63. Interclick expends substantial resources to augment its profile database by merging information about consumers' online and offline shopping, interests, and characteristics. Interclick acquires this additional information from data brokers.

64. The information Interclick acquires from data brokers and merges with its database of individual consumer profiles includes consumer household-level information regarding age, income, education, family circumstances, location, lifestyle, shopping patterns, and interests, and including SKU-level purchasing information.

65. Interclick augmented its profile database with individual-level information it acquired from Defendants in the process of optimizing and measuring the success of advertising campaigns. For example, Defendants and Interclick cooperated to identify consumers are "hand

raisers” who clicked on an advertisement to visit the advertiser’s website, register to enter the advertisers’ sweepstakes or play online games, or make purchases.

66. Interclick’s profiles are stored and analyzed in a data warehouse designed to allow Interclick to mine and correlate the large volumes of highly granular consumers data it acquires.

67. Interclick significantly increased its data warehousing and analysis capabilities in early 2010. Interclick has stated that it “organizes and values billions of data points daily to construct the most responsive digital audiences for major digital marketers.”

68. Interclick’s compilation and analyses of consumer profile data resulted in the deanonymization of data in consumer profiles such that the profiles constitute consumers’ personally identifiable information.

69. Interclick further augments its consumer profiles with information it scrapes from consumers browser history records while it serves advertisements, by engaging in browser history sniffing.

70. Interclick engages in browser history sniffing on behalf of Defendants to obtain information about entities with whom consumers have communicated and with whom Interclick and Defendants have no affiliation.

71. Defendants and Interclick used browser history sniffing to identify Defendants’ competitors with whom consumers communicated as well as websites consumers visited that might indicate consumers’ levels of interest in Defendants’ products and services.

72. Interclick merges the purchased data with the information it acquires through its online contact with consumers to enhance its consumer profiles. All the consumer information Interclick acquired while executing an ad campaign for any one Defendant was merged into In-

terclick's consumer profile database and subsequently used for behavioral targeting on behalf of all Defendants.

73. Defendants' acquisition of consumers' information through browser history sniffing was contrary to standards for Internet communications and interactive advertising.

74. In any given month, Interclick's ad-serving activities allow it to communicate with two-thirds to three-quarters of all U.S. consumers who use the Internet.

75. Because Defendants, including Doe Defendants, represent a wide variety of businesses, Interclick's services on behalf of Defendants allow it to communicate with and profile millions of consumers.

**G. Plaintiff's Experience and Class Consequences**

76. Plaintiff is a U.S. consumer who has frequently used the Internet during the Class Period.

77. On or about late October 2010, Plaintiff examined the contents of her local storage associated with the Adobe Flash Player application on her computer and discovered an LSO set by interclick.com.

78. It is Plaintiff's belief that this object is or is part of a tracking device used by Interclick to monitor and profile her Internet activities.

79. Plaintiff did not expect, receive notice of, or consent to the installation of an Interclick LSO and did not want such a device to be installed on her computer.

80. It was impossible for any website on which Defendants' ads were displayed to consent to Defendants' undisclosed activities. They were not authorized to consent to such circumvention of user controls and commandeering of user resources. Defendant's use of LSOs to monitor Plaintiff's Internet communications exceeded the scope of any authorization that could

have been granted by any publisher on whose web pages Defendant engaged in acquisition of Plaintiff's browser history information.

81. Plaintiff did not expect, receive notice of, or consent to Interclick's performance of browser-history sniffing on her computer and did not want Interclick to engage in such activity.

82. Plaintiff considers information about her online activities to be in the nature of confidential information that she protects from disclosure by periodically deleting cookies.

83. Plaintiff considers information about any website she has visited to be in the nature of confidential information that she does not expect to be available to an unaffiliated website from a different domain.

84. Plaintiff's experience is typical of the experiences of Class Members.

85. Based on reports of Defendants' browser-history sniffing activities, Interclick's role as a major online ad network, the presence of an Interclick LSO on her computer, and the scope of Interclick's communications with the population of U.S. Internet users, and the number and duration of Defendants' online advertising campaigns, Plaintiff believes her web-browsing has been the subjected to Defendants' browser-history sniffing and collection of information using LSOs as tracking devices.

86. Plaintiff did not expect, receive notice of, or consent to Defendants' performance of browser-history sniffing or LSO-based tracking on her computer and did not want Defendants to engage in such activity.

87. Defendant's browser-history sniffing exceeded the scope of any authorization that could have been granted by any publisher on whose web pages Defendant engaged in acquisition of Plaintiff's browser history information.

## **H. Defendants' Lack of Authorization**

88. Defendant's actions in depositing LSOs on consumers' computers, in addition to circumventing consumers' browser controls, affected consumers' reasonable expectations regarding their abilities to control third-party monitoring and information collection in that: (a) many consumers are aware of browser cookies but are unaware of LSOs; (b) consumers browsers are generally equipped with utilities identifying and controlling third-party browser cookies but consumers but have no reasonable means of identifying or managing LSOs, particularly LSOs repurposed by third-party advertising networks of whose presence consumers are unlikely to be aware; (c) to the extent Adobe Corporation purports to offer tools for managing LSOs, such tools reside on Adobe's servers, are proprietary to Adobe, and are not reasonably usable or accessible; (d) unlike browser cookies, which are four kilobytes, LSOs may be up to 100 kilobytes in size; (e) unlike browser cookies which, by default, expire at the end of a consumer's browser session, LSOs have no default expiration; (f) unlike browser cookies, which are stored by and accessible to the consumer through utilities in the consumer's browser or browsers, LSOs are browser-independent; (g) unlike browser cookies, the specifications for the manner in which LSOs can be created and manipulated is controlled by a single vendor, Adobe; (h) unlike browser cookies, Adobe's design of LSOs permits third-parties' cross-domain access; and (i) and unlike browser cookies, Adobe's design of LSOs permits third parties' nontransparent override of consumers' encrypted (HTTPS) web communications.

89. Defendant's actions in depositing and using LSOs and browser-history sniffing code were surreptitious and without notice and so were conducted without authorization and exceeding authorization.

90. Plaintiff and Class Members sought to maintain the secrecy and confidentiality of their personal information assets acquired by Defendant.

91. The confidential character of Plaintiff and Class Members' personal information is further demonstrated by their utilization of browser privacy controls and their reasonable reliance on global standards that protect users from cross-domain activity.

92. The confidential character of Plaintiff and Class Members' personal information is further demonstrated by Interclick's use of surreptitious and deceptive methods to deposit LSOs and performing browser-history sniffing on Plaintiff and Class Members' computers.

93. Defendant has misappropriated Plaintiff and Class Members' personal information.

#### **I. Consequences**

94. Consumers routinely engage in online economic exchanges with the websites they visit by exchanging their personal information for the websites' content and services, thereby reducing the costs consumers would otherwise have to pay.

95. Even when such transactions involve do not involve the transmission of personally identifiable information, but merely *personal* information with which consumers are tracked in supposed anonymity, consumers engage in value-for-value exchanges by providing their information in exchange for content and services.

96. This value-for-value exchange takes place particularly when a website's offerings are supported by advertising revenue, as when Defendants pay to display their advertisements. In such cases, the consumer becomes a participant in what is known as a two-sided business platform. On one side is one customer (the consumer), and on the other side is the advertiser. The website stands in middle as an intermediary, brokering transactions for and among itself and the

occupants of the other sides of the platform. The consumers provide personal information and advertisers pay the website/intermediary for access to the consumers' information. The website's so-called "free" offerings are inducements to increase consumer participation, which, in turn, the website parlays into increased advertising revenue.<sup>2</sup>

97. Because, as alleged herein, Defendants engage in undisclosed and inadequately disclosed data collection from consumers, those consumers do not receive the full value of their exchange. In essence, Defendants raise the price consumers must pay to obtain a website's content services, but instead of telling consumers *or* the website, Defendants simply reach around (or through) the website and into consumers' pockets, extracting their undisclosed premium in the form of consumers' information.

98. Because Defendants impose an undisclosed cost on consumers, by taking more information than they are entitled to take, Defendants' practices impose economic costs on consumers.

99. In addition, the undisclosed privacy and information transfer consequences of Defendants' practices impose costs on consumers in the form of the loss of the opportunity to have entered into value-for-value exchanges with *other* web publishers and third-party advertisers whose business practices better conform to consumers' expectations. This is because consumers use their personal information not only to acquire online offerings; they use it to acquire a better-

---

<sup>2</sup> Two industry organizations that represent online advertising interests acknowledge the value exchange between consumers and websites. The Interactive Advertising Bureau (IAB) recently observed that, without consumers' data, "consumers would encounter a severely diminished experience since they would lose out on the remarkable benefits provided by data sharing. Similarly, the Network Advertising Initiative (NAI) stated, "Instead of requiring visitors to register and pay a subscription fee, the operators of Web offerings subsidize their offerings with various types of advertising." The NAI noted behaviorally targeted ads rely on personal information furnished by consumers such as "registration information reflecting [consumers'] gender, age, or zip code; or alternatively, other potential interests of [consumers] inferred from prior Web activity, either on the publisher's site or elsewhere on the web."<sup>2</sup> Thus, advertising industry spokespersons have acknowledged that consumers obtain value online because they exchange something of value—their personal information.

value exchange by choosing among competing websites. Given that they have choices in where they will engage in these value-for-value exchanges, Defendants' failure adequately to disclose its information practices and using its lack of disclosure to take consumers' information, Defendants imposes a real opportunity cost on consumers.

100. Likewise, Defendants' lack of disclosure coupled with its taking of information imposes costs on consumers who would otherwise have exercised their rights to utilize the economic value of their information by declining to exchange it with Defendants or any competitor—foregoing online offerings entirely. Consumers routinely exercise such choices by electing whether to visit websites or download products, or whether to set browser filters that limit how online websites can collect information. These, too, are decisions predicated on consumers' recognition and exercise of the value of their information.

101. Consumers' information, which they use as an asset of economic value in the ways described above, has value as an asset in the information marketplace. Online websites have proven the value of consumers' information through those websites' own business models, such as the fact that an online website acquires revenue by providing consumer data to ad-delivery entities, or by allowing such entities to access consumers and acquire their information online. These practices have created an active market in which consumer information has a discernable price.

102. In addition, the information marketplace includes opportunities for consumers themselves to market their information directly to online websites and advertisers and control the transfer of their information, with services such as allow.com (UK) (“[p]ersonal information like your name and address is being traded for profit everyday. Now you can help stop this trade and

turn your data into cash for yourself with ALLOW's new, free service"); personal.com ("[o]wn, manage, and share your personal information"); and selectout.org.

103. Thus, Defendants' conduct alleged in this complaint constituted an ongoing course of conduct that harmed Plaintiff and consumers in general, and caused them to incur financial losses, in that Defendants, without authorization, acquired the personal information of Plaintiff and Class Members, which information has economic value to Plaintiff and Class Members, causing them to incur costs in the form of information taken and opportunity costs in the form of uses of the economic value of their information of which Defendants deprived them.

104. Defendants realized significant economic benefits from the conduct described above. Defendants' purpose in acquiring consumers' data is to advance their commercial interests. Defendants' were engaged in the business of selecting and displaying advertisements and did so based, in part, on the data they individual consumers, which they used for ad-serving purposes.

105. Defendants deprived consumers of their right to make adequately informed decisions about whether they would do business with Defendants or one of its competitors.

106. By that same conduct, Defendants imposed on consumers the undisclosed opportunity costs of their choosing to do business with Defendants.

107. The costs and harms described above are aggravated by Defendants' continued retention and commercial use of the improperly acquired consumer data.

108. Defendants' conduct caused economic loss to Plaintiff in that, as discussed above, her personal information has discernable value, both to Defendant and to Plaintiff.

109. Defendants deprived Plaintiff of and/or diminished the economic value of her personal information.

110. Defendants used Plaintiff's personal information for their own economic benefit.

111. In addition to dispossessing Plaintiff and Class Members of the value of their personal information, Defendants dispossessed Plaintiff and Class Members of the value of their computers and computer-related services, as detailed below.

112. Consumers pay for computers capable of a particular level of processing speed.

113. Consumers pay for Internet connectivity services of a particular level of transmission speed.

114. Defendants undisclosed and unauthorized transmissions to Plaintiffs and Class Members computers usurped computer and connectivity resources to which Defendants were not entitled, diminishing the performance of Plaintiffs and Class Members computer processing and connectivity.

115. In particular, Defendants' actions caused diminutions in processing and connectivity performance because, not only were their actions undisclosed and unexpected, their methods of information collection were more resource-intensive than expected, cookie-based or other routinely employed and reasonably expected collection methods. Defendants' use of Adobe LSOs involved the transfer of larger files than cookies. Defendants' use of browser history sniffing code involved either the transmission, back to Defendants, of the tracking collected through browser history sniffing (which ranged from an inspection to determine whether consumers had visited anywhere from 46 to over 220 websites); or, even if Defendants did not collect the detailed browser history data, their use of it to serve a behaviorally targeted advertisement required an additional "round trip" transmission from the consumers' computer, back to Interclick's server to fetch the custom-selected ad, and then back to the consumer's computer to display the ad. In either event, the consumer paid for the trip.

116. This use of consumers' resources is especially injurious for consumers whose Internet service providers impose a bandwidth cap or "bit cap" or download quota. In these cases, consumers suffered not only the diminished performance during Defendants' communications but also suffered the unavailability of services, or diminished availability of services, because of the services unexpectedly and unauthorizedly used by Defendants.

117. As Interclick is in the business of monitoring and counting which ads it serves to which consumers and with what frequency, and accounting for its activities and charging advertisers, on the one hand, and paying fees to websites, on the other, the harm wrought by Defendants' activities can be quantified, in part, by an examination of Defendants' records. In addition, the service levels and expected transfer rates for Plaintiff and Class Members' are ascertainable from the records of their Internet service providers.

118. It should be noted that, according to Alexa.com, which monitors and ranks websites by traffic activity, 49 percent of all websites monitored by Alexa loaded faster than Interclick's.

119. Plaintiff's experience is typical of the experiences of Class Members.

120. The aggregated loss and damage sustained by the Class, as defined herein, includes economic loss with an aggregated value of at least \$5,000 during a one-year period.

121. Defendants perpetrated the acts and omissions set forth in this complaint through an organized campaign of deployment, which constituted a single act.

122. Based on Defendants' actions in acquiring Plaintiff's and Class Members' personal information, an implied contract existed between Defendants and Class Members, to which Defendants' assent may be fairly inferred, and under which contract Defendants were unjustly enriched.

123. Plaintiff and Class Members have been harmed by Defendants' deceptive acquisition of their personal information in the loss of their rights to use, share, and maintain the confidentiality of their information, each according to his or her own discretion.

## V. CLASS ALLEGATIONS

124. Pursuant to the Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), Plaintiff brings this action as a class action on behalf of herself and all others similarly situated as members of the Classes, defined as follows:

**National Class:** All persons residing in the United States who, since June 1, 2007, were profiled by or whose profiles were used by interCLICK, Inc. in the course of its activities with and on behalf of Defendants.

**New York Sub-Class:** All persons residing in New York who, since June 1, 2007, were profiled by or whose profiles were used by interCLICK, Inc. in the course of its activities with and on behalf of Defendants.

125. Excluded from the Classes are Defendants, their legal representatives, assigns, and successors, and any entities in which Defendants have controlling interests. Also excluded is the judge to whom this case is assigned and the judge's immediate family.

126. The "Class Period" is June 1, 2007 to the present.

127. Plaintiff reserves the right to revise these definitions of the Classes based on facts learned in the course of litigating this matter.

128. The Classes consist of millions of individuals and other entities, making joinder impractical.

129. The claims of Plaintiff are typical of the claims of all other Class Members.

130. Plaintiff will fairly and adequately represent the interests of the other Class Members. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and her counsel are committed to prosecuting this action vigorously

on behalf of Class Members and have the financial resources to do so. Neither Plaintiff nor her counsel has any interests adverse to those of the other Class Members.

131. Absent a class action, most Class Members would find the cost of litigating their claims to be prohibitive and would have no effective remedy.

132. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants, and promotes consistency and efficiency of adjudication.

133. Defendant has acted and failed to act on grounds generally applicable to Plaintiff and other Class Members, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members.

134. The factual and legal bases of Defendants' liability to Plaintiff and other Class Members are the same, resulting in injury to Plaintiff and all of the other Class Members. Plaintiff and other Class Members have all suffered harm and damages as a result of Defendants' wrongful conduct.

135. There are many questions of law and fact common to Plaintiff and the Class Members and those questions predominate over any questions that may affect individual Class Members. Common questions for the Class include, but are not limited to the following:

- a. whether Defendants, without authorization, performed browser-history sniffing on computers to which Class Members enjoyed rights of possession superior to those of Defendants;
- b. whether Defendants, without authorization, created personally identifiable profiles of Class Members;

c. Whether Defendants violated: (i) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (ii) Section 349 of the New York General Business Law; and (iii) other violations of common law.

d. Whether Defendants misappropriated valuable information assets of Class Members;

e. Whether Defendants created or caused or facilitated the creation of personally identifiable consumer profiles of Class Members;

f. Whether Defendants continue to retain and/or make use of, through Inter-click, valuable information assets from and about Class Members;

g. What uses of such information were exercised and continue to be exercised by Defendants;

h. Whether Defendants invaded the privacy of Class Members;

i. Whether Defendants' actions constituted trespass to personal property;

j. Whether Defendants' actions evince an implied contract between Defendants and Class Members; and

k. Whether Defendants have been unjustly enriched.

136. The questions of law and fact common to Class Members predominate over any questions affecting only individual members, and a class action is superior to all other available methods for the fair and efficient adjudication of this controversy.

## **VI. CLAIMS FOR RELIEF**

137. Based on the foregoing allegations, Plaintiff's claims for relief include the following:

**FIRST CLAIM FOR RELIEF**  
**Violations of the Computer Fraud and Abuse Act,**  
**18 U.S.C § 1030, *et seq.***  
**(On Behalf of Plaintiff and the National Class)**

138. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

139. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, referred to as “CFAA,” regulates fraud and related activity in connection with computers, and makes it unlawful to intentionally access a computer used for interstate commerce or communication, without authorization or by exceeding authorized access to such a computer, thereby obtaining information from such a protected computer, within the meaning of U.S.C. § 1030(a)(2)(C).

140. Defendants violated 18 U.S.C. 1030 by intentionally accessing Plaintiff’s and Class Members’ computers without authorization or by exceeding authorization, thereby obtaining information from such a protected computer.

141. The CFAA, 18 U.S.C. § 1030(g) provides a civil cause of action to any person who suffers damage or loss by reason of a violation of CFAA.

142. The CFAA, 18 U.S.C. § 1030(a)(5)(A) makes it unlawful to knowingly cause the transmission of a program, information, code, or command and as a result of such conduct, intentionally cause damage without authorization, to a protected computer of a loss to one or more persons during any one-year period aggregating at least \$5,000 in value.

143. Plaintiff’s and Class Members computers each constitute a “protected computer . . . which is used in interstate commerce and/or communication” within the meaning of 18 U.S.C. § 1030(e)(2)(B).

144. Defendants violated 18 U.S.C. § 1030(a)(5)(A) by knowingly causing the transmission of a command to be downloaded to Plaintiff’s and Class Members’ computers, which

are protected computers as defined above. By storing LSOs and executing browser-history sniffing code to access, collect, and transmit details of Plaintiff's and Class Members' web activities and communications, Defendants intentionally caused damage without authorization to those Class Members' computers by impairing the integrity of the computers.

145. Defendants violated 18 U.S.C. 1030(a)(5)(B) by intentionally accessing Plaintiff's and Class Members' protected computers without authorization, and as a result of such conduct, recklessly caused damage to Plaintiff's and Class Members computers by impairing the integrity of data and/or system and/or information.

146. Defendants violated 18 U.S.C. 1030(a)(5)(C) by intentionally accessing Plaintiff's and Class Members' protected computers without authorization, and as a result of such conduct, causing damage and loss to Plaintiff and Class Members.

147. Plaintiff and Class Members suffered damage by reason of these violations, as defined in 18 U.S.C. 1030(e)(8), by the "impairment to the integrity or availability of data, a program, a system or information."

148. Plaintiff and Class Members have suffered loss by reason of these violations, including, without limitation, violation of the right of privacy, and disclosure of personal information that is otherwise private, confidential, and not of public record.

149. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered harms and losses that include those described in paragraphs 94 through 123, above.

150. Defendants' unlawful access to Plaintiffs' and Class Members' computers through the use of repurposed LSOs and browser history sniffing code constituted a single act

that resulted in an aggregated loss to Plaintiff and the Class of at least \$5,000 within a one-year period.

151. Therefore, Plaintiffs and the Class are entitled to compensatory damages.

152. Defendants' unlawful access to Plaintiff's and Class Members' computers and personal information has caused Plaintiff and Class Members irreparable injury. Unless restrained and enjoined, Defendants will continue to commit such acts. Plaintiff's and Class Members' remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Plaintiff and Class Members to remedies including injunctive relief as provided by 18 U.S.C. § 1030(g).

**SECOND CLAIM FOR RELIEF**  
**Violation of Section 349 of New York General Business Law**  
**Deceptive Acts and Practices**  
**(On Behalf of Plaintiff and the New York Sub-Class)**

153. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

154. Defendants' actions alleged herein constitute unlawful, unfair, deceptive, and fraudulent business practices.

155. Defendants' conduct constitutes acts, uses and/or employment by and/or their agents or employees of deception, fraud, unconscionable and unfair commercial practices, false pretenses, false promises, misrepresentations and/or the knowing concealment, suppression, and/or omission of material facts with the intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of services, and with the subsequent performance of services and transactions, in violation of section 349 of New York's General Business Law.

156. Defendants' acts and omissions were generally directed at the consuming public in that the fundamental nature of their activity was to obtain information from consumers and to do so despite consumers' privacy and security settings, to do so despite the character and existence of agreements between consumers and intermediary websites, to use the obtained information to profile consumers, to serve ads during their interactions, and to retain profile information and enhance it using external data sources for use in the future serving of ads to consumers. In essence, the entire scope of Defendants' activities complained of herein consisted of obtaining information from, and about consumers, and delivering advertising to consumers. These activities are therefore consumer-oriented.

157. Defendants' conduct was materially misleading in that (a) consumers reasonably expected that their browser, privacy and security controls would in fact control the kinds of tracking and profiling performed by Defendants; (b) consumers reasonably expected that, subject to their controls, any information collection would be performed through the use of cookies or other generally accepted data collection mechanisms, and not through technologies such as repurposed LSOs and browser history sniffing, that by their very nature were designed to operate outside consumers' expectations, awareness and ability to detect; (c) the very fact that consumers had implemented privacy and security controls demonstrates the materiality of Defendants' misrepresentations and omissions, through its actions, and through its data collection and use; (d) Defendants' very use of such detection evading technologies demonstrates Defendants' own recognition of the materiality of its own misrepresentations and omissions in as much as if their practices were immaterial to consumers, Defendants would not have gone to such lengths to hide them. The materiality of Defendants' misrepresentations and omissions assumes even greater weight in light of the fact that not only did Defendants thwart consumers' expectations and ex-

press limitations, Defendants purpose, which Defendants consistently achieved, was to repeatedly and surreptitiously take consumers' personal information, which was of value to those consumers.

158. The unfair and deceptive trade acts and practices of Defendant have directly, foreseeably, and proximately caused damages and injury to Plaintiff and other members of the Class.

159. Defendants' violations of Section 349 of New York's General Business Law have damaged Plaintiff and other Class Members, and threaten additional injury if the violations continue.

160. Defendants' acts and omissions, including Defendants' misrepresentations, have caused harm to Class Members in that Class Members have suffered the loss of privacy through the exposure of the personal and private information and evasion of privacy controls on their computers as described more fully above in paragraphs 94 through 123, above

161. Defendants knowingly and willfully violated Section 349 of the New York General Business Law.

162. Plaintiff and Class Members have no adequate remedy at law.

163. Pursuant to Section 349 of the New York General Business Law, Plaintiff seeks an order to enjoin Defendants from such future conduct.

164. Pursuant to Section 349 of the New York General Business Law, Plaintiff seeks actual, statutory, and treble damages, costs and expenses, pre and post-judgment interest, and attorneys' fees.

**THIRD CLAIM FOR RELIEF**  
**Trespass to Personal Property/Chattels**  
**(On Behalf of Plaintiff and the National Class)**

165. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

166. By engaging in the acts alleged in this Complaint, Defendants intentionally, and without justification or consent, physically interfered with the use and enjoyment of personal property in Plaintiff and Class Members' possession, thereby causing harm to Plaintiff and Class Members.

167. Plaintiff and Class Members, at all times relevant to this action, were the owners and/or possessors of computers and of their information collected through Defendants' use of Flash LSOs and browsing history sniffing code placed on Plaintiff's and Class Member's computers.

168. Defendants dispossessed Plaintiffs and Class Members of the use of their computers, or parts of them, for a substantial time by commandeering those resources for their own purposes.

169. Defendants dispossessed Plaintiffs and Class Members of the value of their personal information by using tracking technologies to access such information.

170. Defendants impaired the condition, quality, and value of users' computers by its installation and use of Flash LSOs and browser history sniffing code, which constituted an ongoing alteration to users' computers and which affected the performance of their browsers on an ongoing basis, circumventing users' browser privacy controls and causing users' browsers to transmit information to Defendants to which Defendants were not entitled.

171. Plaintiffs and Class Members each had and have a legally protected economic interest in their personal information.

172. Users sustained harm as a result of Defendants' actions as described in paragraphs in paragraphs 94 through 123, above.

173. Without Plaintiff and Class Members' consent, or in excess of any consent given, Defendants knowingly and intentionally accessed Plaintiff and Class Members' property and caused injury to Plaintiff and the Members of the Class.

174. Defendants engaged in deception and concealment in order to gain access to Plaintiff and Class Members' computers and personal information.

175. Defendants' installation and operation of the LSOs and execution of browser-history sniffing code interfered and/or intermeddled with Plaintiff and Class Members' computers, including by circumventing their controls designed to prevent the information collection effected by Defendants. Such use, interference and/or intermeddling was without consent, or in the alternative, in excess of consent.

176. Defendants' installation and operation of the LSOs and execution of browser-history sniffing code impaired the condition and value of Plaintiff and Class Members' computers.

177. Defendants' trespass to chattels, nuisance, and interference caused real and substantial damage to Plaintiff and Class Members.

178. As a direct and proximate result of Defendants' trespass to chattels, nuisance, interference and unauthorized access of and intermeddling with Plaintiff's and Class Member's property, Defendants have injured and impaired in the condition and value of Class Members' computers as follows:

179. Plaintiff and Class Members have no adequate remedy at law.

180. Plaintiff, individually and on behalf of the Class, seeks injunctive relief restraining Defendants from committing trespass to chattels, to purge the data, and damages.

**FOURTH CLAIM FOR RELIEF**  
**Breach of Implied Contract**  
**(On Behalf of Plaintiff and the National Class)**

181. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

182. The common law prohibits the breaches of contract, including a contract implied under the circumstances of a relationship between parties, such that a breach results in the unjust and inequitable enrichment of one party at the expense of another.

183. Plaintiff and Class Members provided their personal information in good faith to websites (publishers), reasonably expected that such information would be exchanged with the advertisers and that Plaintiff and Class Members would in turn receive the goods and services offered by such websites.

184. However, Defendants, using their access to the Plaintiff's and Class Members' personal information, accorded to it by the websites, but without the websites' knowledge and consent, took more information than that to which it was entitled, and furthermore, did so by bypassing Plaintiff's and Class Member's privacy and security controls, effectively nullifying such controls, and by executing unexpected rogue code that conducted an unexpected and unauthorized inspection of Plaintiff's and Class Member's browsing history.

185. Because of the multi-platform character of the business model involving Plaintiff and Class Members, the websites (publishers), and the advertisers, Plaintiff and Class Member's relationship with the advertisers in the context of that multi-platform model was one of claim-

ant/provider of information assets to purchaser/user of information assets through the intercessory role of the web site or publisher. Accordingly, Plaintiff and Class Members are entitled to recover the value of the information provided.

186. By engaging in the acts alleged in this complaint, including the deposit and manipulation of LSOs and the execution of browser-history sniffing code by which Defendants collected Plaintiff's and Class Members' personal information without authorization or consent of Plaintiff and Class Members, Defendants unjustly enriched themselves at the expense of Plaintiff and Class Members by appropriating their personal information, through surreptitious means and without their consent, for its own gain and to the detriment of Plaintiff and Class Members' interest in maintaining the confidentiality of their information and/or sharing it with parties of their own choosing.

187. Defendants were unjustly enriched at the expense of Plaintiff and Class Members in that Interclick received advertising fees and Defendants realized increased traffic, lead identification, conversion of leads, and in the process, augmentation of their own databases of consumer information.

188. Defendants appreciate and/or have knowledge of said benefits.

189. Under principles of equity and good conscience, Defendants should not be permitted to retain the information and/or revenue that they acquired by virtue of their unlawful conduct. All funds, revenue, and benefits received by Defendants rightfully belong to Plaintiff and the Class, which Defendants have unjustly received as a result of their actions.

190. Plaintiff and Class Members have no adequate remedy at law.

**FIFTH CLAIM FOR RELIEF**  
**Tortious Interference with Contract**  
**(On Behalf of Plaintiff and the National Class)**

191. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

192. The common law prohibits intentional interference in contracts between other parties that cause one of the parties to breach the contract without justification, resulting in damages.

193. When Plaintiff and Class Members visited websites on which Interclick operated, they entered into agreements with the operators of those websites, which agreements included privacy policies and terms of services.

194. Defendants' activities, as described above, were in conflict with the privacy policies and/or terms of use of the websites Plaintiff and Class Members visited, which were valid contracts between Plaintiff and Class Members and the owners/operators of such websites; in particular, the contracts did not provide consent and notice of Defendants' browser history sniffing, profiling, and deanonymization activities and/or use of Flash LSOs as cookie substitutes.

195. Defendants, through Interclick, knew which websites Plaintiff and Class Members, were visiting and interacting with Interclick and, by the same token, knew which websites privacy policies and terms of service constitutes valid contracts between Plaintiffs and Class Members and such websites.

196. Defendants intended to procure, and in fact did procure, websites to breach their privacy policies and terms of use with Plaintiff and Class Members, without any justification, by causing Interclick to engage in browser history sniffing, profiling, and deanonymization activities, which rendered such websites' privacy commitments false and misleading.

197. As a direct and proximate result of such breaches of contract, Plaintiffs and Class Members were harmed and suffered damages as described above in paragraphs 94 through 123, above

198. Plaintiff and Class Members have no adequate remedy at law.

## **VII. DEMAND FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, prays for judgment against Defendants and that the Court may:

- A. certify this case as a Class action on behalf of the Classes defined above, appoint Plaintiff as Class representative, and appoint her counsel as Class counsel;
- B. declare that Defendants' actions, as set forth above, violate the Computer Fraud and Abuse Act; the New York General Business Law, Section 349; and such common law torts as are alleged above;
- C. award injunctive and equitable relief as applicable to the Class *mutatis mutandis*, including:
  - i. prohibiting Defendants from engaging in the acts alleged above;
  - ii. requiring Defendants to provide reasonable notice and choice to consumers regarding Defendants' data collection, profiling, merger, and de-anonymization activities;
  - iii. requiring Defendants to disgorge to Plaintiff and Class Members or to whomever the Court deems appropriate all of Defendants' ill-gotten gains;
  - iv. requiring Defendants to delete all data from and about Plaintiff and Class Members that it collected and/or acquired from third parties through the acts alleged above;

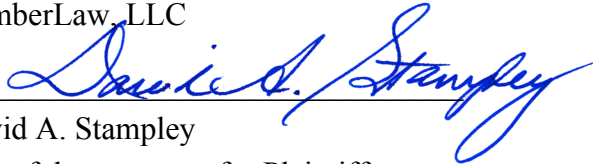
- v. requiring Defendants to provide Plaintiff and other Class Members reasonable means to decline, permanently, participation in Defendants' collection of data from and about them;
  - vi. awarding Plaintiff and Class Members full restitution of all benefits wrongfully acquired by Defendants through the wrongful conduct alleged above; and
  - vii. ordering an accounting and constructive trust to be imposed on the data from and about Plaintiff and Class Members and on funds or other assets obtained by unlawful means as alleged above, to avoid dissipation, fraudulent transfers, and/or concealment of such assets by Defendants;
- D. award damages, including statutory and treble damages where applicable, to Plaintiff and Class Members in an amount to be determined at trial;
- E. award restitution against Defendants for all money to which Plaintiff and the Classes are entitled in equity;
- F. restrain, by preliminary and permanent injunction, Defendants, its officers, agents, servants, employees, and attorneys, and those participating with them in active concert, from identifying Plaintiff and Class Members online, whether by personal or pseudonymous identifiers, and from monitoring, accessing, collecting, transmitting, and merging with data from other sources any information from or about Plaintiff and Class Members;
- G. award Plaintiff and the Class their reasonable litigation expenses and attorneys' fees; pre- and post-judgment interest to the extent allowable;
- H. and such other relief as this Court deems just and proper.

### VIII. JURY TRIAL DEMAND

Plaintiff hereby demands a trial by jury of all issues so triable.

Dated: March 21, 2011

Respectfully submitted,  
KamberLaw, LLC

By:   
David A. Stampley

One of the attorneys for Plaintiff,  
individually and on behalf of a class of  
similarly situated individuals

Scott A. Kamber  
skamber@kamberlaw.com  
KamberLaw, LLC  
100 Wall Street, 23rd Floor  
New York, New York 10005  
Telephone: (212) 920-3072  
Facsimile: (212) 920-3081

David A. Stampley  
dstampley@kamberlaw.com  
KamberLaw, LLC  
100 Wall Street, 23rd Floor  
New York, New York 10005  
Telephone: (212) 920-3072  
Facsimile: (212) 920-3081

Joseph H. Malley (not admitted)  
malleylaw@gmail.com  
Law Office of Joseph H. Malley  
1045 North Zang Boulevard  
Dallas, Texas 75208  
Telephone: (214) 943-6100

Robert K. Shelquist (not admitted)  
Lockridge Grindal Nauen P.L.L.P.  
100 Washington Avenue South, Suite 2200  
Minneapolis, Minnesota 55401-2159  
Telephone: (612) 339-6900  
Facsimile: (612) 339-0981